PROFESSIONAL SERVICES

Creating Sustainable Business Advantage

PKI Vendor Analysis and RFP Recommendations - Updated

July 14, 2000

Prepared for:
Ken Adrian
State of Iowa, IT Department
ITS 'B' Level, Hoover Building
Des Moines, IA 50319

Prepared by:
Professional Services
10 Fawcett Street
Cambridge, MA 02138

Table of Contents

1.0 Introduction

This document and the associated Excel spreadsheet contain the following analyses:

- An comparison of PKI vendors and the features they provide, with explanatory text here, that can be used to help determine which vendors the State wishes to contact.

- A summary of requirements, based on State needs and available vendor features, that can be used as guidance in writing the Request for Proposal (RFP) that the State expects to produce soon.

These documents comprise the final deliverable in the current consulting engagement by Baltimore Technologies' Professional Services for the State of Iowa.

The vendor product/service analysis is provided in the form of an Excel spreadsheet, which the text of this Word document accompanies and explains. The spreadsheet contains scores and suggested weights that can be easily reconfigured by the State for changing assumptions. The text in this Word document explains the spreadsheet entries in more depth, for understanding and to support the eventual RFP.

2.0 Explanation of Spreadsheet, and RFP Requirements

This section walks through the spreadsheet by column and row, explaining the categories and entries. It also provides more detail for some important spreadsheet entries. The State is of course free to change any parameter values or other assumptions for its own analyses.

2.1 Columns

The spreadsheet columns list the major requirements (column A) and a number for each that reflects its importance (column B). The remaining columns, two per PKI vendor, then describe briefly how well that vendor's products meet each requirement, and provide a numeric score. These scores are somewhat arbitrary, and the State can change them. However, the score granted for a given requirement should normally be no greater than the maximum in column B, as a guideline.

2.2 Vendor List and Snapshot Summary: Rows 3 and 4

These rows list each vendor, followed by a brief summary of a few key characteristics of that vendor. They mostly offer Certification Authority (CA) and other related PKI products. However, the last two vendors are the significant CA service providers who offer outsourced CA support that would allow the State to avoid or postpone building its own CA facility. This vendor list includes all significant currently active CA product or service providers. Although a few other small CA vendors may be available, we do not recommend that the State consider them because of doubts as to their viability or commitment to PKI. (In fact, even some of the listed vendors may have issues on this point, as noted in the spreadsheet and the present document.)

CA product vendors consist of:

- Baltimore Technologies, specifically the product vendor part of the company that offers both CA and PKI-enabled application products. The CA product is called UniCERT. (Note: Professional Services is a semi-independent part of Baltimore Technologies that was part of BBN and then GTE CyberTrust before being acquired by Batlimore a few months ago.)
- Entrust, a company rather like Baltimore Technologies but with a greater emphasis on their non-CA product line.
- Microsoft, whose new Windows 2000 operating system includes a simple CA and PKI support functions. This is likely not appropriate for the State at this time because it is a first-generation product and only applies to Windows 2000. However it is included here because it bears watching if Microsoft continues to develop it, and some departments in the State may be interested in it for their own internal use.
- RSA Security's KEON product. This is also a first-generation product that bears watching. It appears to be generating the most interest as a low-level PKI system that can be retrofitted into existing legacy systems.
- CertCo, which is a smaller specialty PKI company perhaps best known as the provider of the Secure Electronic Transaction (SET) Root CA. CertCo's future direction appears somewhat uncertain at this time: it recently obtained a new CEO and CFO and several vice presidents, and it may be looking for niche markets in the PKI area.
- Xcert, which is another smaller company that is trying to remain a full-feature CA and PKI vendor.

- Cylink, which is primarily a network encryption products company but also has a small unit providing a CA product. They have worked with the US Postal Service but mentioned no other customers when asked. The State of Iowa may wish to contact the US Postal Service for their opinion of Cylink's work.

CA service providers consist of:

- Baltimore Technologies' CA Hosting Service, which is an outsourced CA service provider. This unit was previously part of GTE CyberTrust. It is adding UniCERT CAs, and will soon use the "best of breed" combination of UniCERT and CyberTrust features.
- VeriSign, the other major CA service provider, which is rather like Baltimore's CA Hosting Service.
- ID Certify, a small company that provides basic CA services to the State of Washington, and just received a contract with the State of Minnesota to develop more advanced services.
- Digital Signature Trust, a small subsidiary of the Zion National Bank that provides CA services to the State of Utah. They did not respond to a request for information as of this writing, so the data here is based on their web site and some older information, and may be somewhat incomplete.

2.3 Requirements and How Met by Vendors: Rows 5 through 33

The requirements are listed roughly in order of importance with one exception (applications) noted below. Thus those with greater numeric importance weights are listed first. Those requirements that should probably be included as relatively firm requirements in the eventual RFP are tagged with an asterisk (*) for easy reference. Non-tagged requirements may be "nice to have" but might be considered optional. The final set of rows, many of which are again rather important, show the various PKI-enabled applications supported by each vendor, either via their own product line or by products of other companies with which the PKI vendor has partnered. Important issues relating to the specific requirements, and how well they are met by the different vendors, are summarized below. As in the spreadsheet, requirements that we recommend be firm if at all possible are noted with an asterisk below; the rest may be optional. Note that many of these requirements are met by almost all CAs, because the PKI industry is becoming more standardized, and because a feature in demand by customers and met by one CA is soon matched by others due to competitive pressures.

- * Scalability (row 6): The State will eventually support a rather large PKI community, so any CA must be prepared to support at least 1 million certificates of various types. This is not a problem for high-end CAs such as CyberTrust (now Baltimore) and VeriSign, but some caution may be appropriate for other vendors that grew out of a small-enterprise model or do not have a proven track record. This is a difficult area to evaluate, as every vendor claims good scalability. The best advice may be to ask for a presently operating large system and talk to the customer who bought it.
- * Interoperability (row 7): CAs must work with a variety of PKI-enabled applications, most of which the CA cannot control. Thus partnerships with PKI application vendors are essential. Interoperability also requires adherence to well-accepted standards.
- * Viability, track record and size (row 8): These entries attempt to estimate how viable the vendor is in the CA/PKI arena, both regarding size and past record. Of course, no company is likely to admit to being in any way non-viable, so the State

will have to ask for proof (including listing of recent customers) and draw its own conclusions.

- * Multi-level CA hierarchy (row 9): As explained in earlier deliverables, it is important to have at least two levels of CA: a root CA that is kept offline, and operational Subordinate CAs that are connected to the Internet to provide certificates to end users. All significant CAs now support this feature.
- * Certificate format flexibility (row 10): The State will have to provide certificates whose exact structure is still somewhat uncertain. Any CA vendor will have to support at least the common name fields and extensions that were described in the earlier PKI Architecture document. Most CA vendors now support all the original X.509 fields/extensions, and most of the newer PKIX extensions being developed by the Internet Engineering Task Force (IETF). The important extensions are listed in the spreadsheet and have been discussed in the PKI Architecture deliverable.
- * Registration Support (row 11): The PKI Architecture document listed multiple certificate authorization/approval methods that should be supported if possible, including manual RAs, automated RAs, and a pre-authorized user list. Registration data, which often does not go into the certificate itself, is needed, including in many cases a "shared secret". Multiple remote RAs must also be supported for convenience and scalability.
- * LDAP interface (row 12): This is the standard interface between a CA and a directory that stores certificates and certificate revocation lists (CRLs). This interface is now supported for virtually all CAs and many other PKI products.
- * Cross-certification support (row 13): This is needed if the State ever wishes to interact on a peer-to-peer basis with other states or Federal government PKI systems. Most CAs support this by the exchange of PKCS#10 certificate requests and installation of the resulting X.509 certificates.
- * Separate encryption certificates (row 14): This may be needed if the functions of signature and encryption are separated, particularly if there is a need to back up encryption keys to protect later decryption of files. Again, this has become almost standard in the PKI industry.
- * Support for hardware cryptodevices at the CA (row 15): For good security, it is essential that a CA's keys be generated and stored in a secure hardware device. All significant CAs offer this as standard practice now.
- Reports (row 16): A CA must provide summary reports of the status of certificate requests, certificates, and CRLs. This is needed for billing, audits, etc. This is often done via a secure internal database (most often Oracle) that can be accessed by cleared CA staff. A basic fixed set of appropriate reports is vital (*), and it is desirable but optional to have configurable reports that CA staff can create, for example by SQL queries to the database.
- * Smartcard or token support (row 17): It is important to be able to store high-value certificates (for example RAs' own certificates used to access the CA) on hardware tokens such as smart cards. Fortunately, this is seldom difficult for the CA because the token vendors provide the interface to the client (browser, email client, etc.) All that is needed usually is a simple test to verify the interface.
- Both CA product and hosting service (row 18): There is some advantage to having compatible service and product offerings, as this allows a customer to start with a CA service in the interest of saving time and money, while still migrating to a similar CA product later. This is not essential, but may be useful to the State in planning for the future. Two vendor combinations may support this at present: the Baltimore Technologies' CA Hosting Service and UniCERT CA product, and (possibly) the

VeriSign CA service and the somewhat similar RSA KEON CA based on VeriSign software licensed by RSA.

- * (essential for CA outsourcing) Various requirements for hosting services (row 19): A good CA service must meet many requirements, particularly for security, because the State's reputation and PKI viability is at stake. These are all listed together here because the only two major CA service providers (mentioned in the previous bullet) meet all necessary requirements and have a proven track record. Please refer to the spreadsheet and the PKI Requirements Assessment for further details.
- Certificate revocation (row 20): There are various ways to notify interested parties when certificates are revoked. The original method is via CRL posting (*) which should be required. A new approach which is desirable is via the Online Certificate Status Protocol (OCSP) interface to an OCSP responder (server). Also desirable but not essential is the ability to put a certificate on hold, as a temporary reversible revocation, while considering its final disposition.
- RA approval before or after the certificate request is sent to the CA (row 21): The RA function can be done before or after the CA receives the end user's certificate request. Either is workable in most systems, but it is ideal if both are available.
- Available root that is embedded in major applications such as browsers, web servers and email (row 22): This is not essential, but if such a root is available, it may save a step when users set up their PKI applications. Otherwise a root may have to be embedded. An example of such a root is Baltimore Technologies' OmniRoot; some other CAs also offer such support as shown here. (This is a moot point if the State decides to use only a State of Iowa root, not tied to any other root.)
- Certificate renewal (row 23): A special certificate renewal process is not essential; users can just apply for a new certificate as they did the old one when that expires. However, there are operational advantages to a special renewal process: being notified of an impending expiration, having the form (most of which will not change) filled out for the user, using the old key for verification and possibly even as the key being certified, and/or avoiding re-authorization (approval) of the certificate request if that is felt to be unnecessary.
- Multi-platform support (row 24): There can occasionally be advantages to a CA being available in both UNIX (e.g. Solaris) and Windows (typically NT 4.0 at this time). This can simplify upgrades in some cases.
- Biometric support (row 25): There has been discussion for some time of using biometric identification such as fingerprint scanning in addition to digital signatures and certificates. Unfortunately, there is a lack of standards in the biometric industry, and in its interface to the PKI industry is also not defined, so no vendor can realistically offer a standards-based solution guaranteed to work in the future. However, a CA might at least offer a special certificate field or extension, which could be defined by the State, for future growth in this area.
- Toolkits (row 26): Toolkits provided by a PKI vendor can be useful for preparing applications to use certificates provided by the CA. This is most likely to be available with CAs that have strong partnership arrangements with application vendors, or perhaps that offer their own applications.
- Certificate support for specific applications (rows 27 through 33): These are applications, some essential as shown by asterisks and others less so, that may be useful to the State. A CA vendor should show the ability to work in real world environments with those applications that are important to the State. The compatible applications should include at least the dominant off-the-shelf programs in that area, and may also include value-added enhancements or alternatives provided by the PKI

vendor or a third party. They include, as discussed in the spreadsheet details and previous deliverables:

- * Access control, the primary application identified in discussions with various State agencies
- * Secure e-mail via S/MIME, the accepted standard.
- * Web browsers and web servers via SSL, the accepted standard
- Virtual private network (VPN) support via IPSec, the accepted standard.
- File signing and/or encryption, and web form signing and/or encryption, with key recovery as a common supporting capability
- Other applications, as noted in the spreadsheet and described in previous deliverables

2.4 Total Score: Row 34

This row sums the scores, bounded by the suggested maximum score available for each requirement based on its importance. This score is a general indication of the capabilities of different PKI products and services. However, it should not be given undue importance. The relative importance of requirements may change. Also, some requirements may be so important as to be essential, and failing one or more such requirements may eliminate a vendor from further consideration. Finally, it can be noted that there is often not a large variation in most scores, because all CA and PKI products considered for this study are basically sound products with similar feature sets. The State can experiment with the spreadsheet as desired to see which vendors appear interesting, but it probably makes sense to contact all vendors on this list. One exception may be Microsoft's low-end CA, partly because they do not consider Windows 2000 primarily a PKI product (so will give no support), and the State may not wish to standardize on Windows 2000 in the near future. Similarly, the Netscape low-end CA is probably unsuitable as it is usable only with Netscape products, and has poor support. The status of CertCo, and perhaps Xcert as well, should also be determined at the time of the RFP. The three vendors suggested by the State of Iowa for consideration are not significant players in the commercial marketplace, and there is some question about scalability or access control application support, but they may still be worth contacting because they work for other government agencies: Cylink (US Postal Service), ID Certify (states of Washington and Minnesota) and Digital Signature Trust (State of Utah). One CA "vendor" that we do not recommend is IBM, which has a history of announcing PKI products such as CAs and then not delivering, and whose PKI direction is very uncertain according to some recent IBM employees.